AMENDMENTS TO THE SPECIFICATION

Please amend the paragraph beginning on page 15, line 13, as follows:

In step 0a of Figure 3, a hardware token 130 is provided. This token will be used to generate private/public key pairs and is pre-loaded with a ~~role~~pedigree certificate and associated private key prior to being provided to the user 132. In step 1 of Figure 3, data regarding the new user 132 is entered into the authoritative database 104. The authoritative database 104 contains information about the members of the enterprise including data necessary to send registration materials to new users. This information may include the home or work addresses, e-mail addresses, telephone or fax numbers, etc. In step 2, the data stored in the authoritative database 104 is periodically frequently replicated to the system directory 108. In step 3, the new user 132 attempts to access one of the enterprise Web servers 138 or 140. Since the new user 132 does not have a signature, the new user 132 does not present a signature to the Web server 140 and accordingly, the Web server 140, in step 5, redirects the new user 132 to the special registration Web page 350. At that point, the new user 132 identifies itself to the special registration Web page 350. In step 6, the special registration Web page 350 queries the directory 108 to obtain information about the new user 132. In step 7, the directory 108 provides information about the new user to the special registration Web page 350.

Please amend the paragraph beginning on page 16, line 18, as follows:

In step 9, the personal registration authority 146 delivers registration information to the new user 132 in a face-to-face meeting. In step 10a, the new user 132 revisits the special registration Web page 350 and can forward the requisite registration information. The special registration of the Web page 350 can only be accessed by using a hardware token 130 that has been pre-loaded with the requisite ~~role~~pedigree certificate and associated private key (from step 0a). In step 11a, the registration Web server 124 signals the registration authority 112 to register the new user 132 possessing the hardware token 130 and in step 12a, the registration authority 112 signals the client platform 128 to generate a private/public key pair on the hardware token 130. Before the public key is sent to the certificate authority, the token can sign the certificate

request before the certificate leaves the token, using the private key. This allows the certification authority to know that the pedigree is valid for the highest level of assurance in the reliability of the key storage mechanism. In step 13, the public key is sent from the client platform 128 to the certificate authority 110, which records the certificate pedigree as a certificate policy object identifier (OID) in the certificate itself. Before signing the certificate, the certification authority validates that the certificate request was signed by the token itself. This makes any Trojan horse attack impossible because only a valid token, with the valid private key for a specific pedigree could have signed the request. In step 14, the certificate authority 110 sends the signed certificate (with public key) to the directory 108. In step 15a, the registration Web server 124 alerts the directory 108 that this certificate was generated on the hardware token 130. The Web server 124 knows this because of the fact that only a user 132 having a hardware token 130 would have been able to access the special version of the registration Web page 350.

Please amend the paragraph beginning on page 18, line 1, as follows:

Thus, if there are one or more categories of computing devices which are able to generate digital certificates and if one wishes to track which certificates in an enterprise were generated by a given category of devices, then in accordance with the present invention, a ~~role~~pedigree certificate is assigned to each category of device for certificates which are to be tracked and these ~~role~~pedigree certificates are pre-loaded in those devices. An automated registration process is provided which allows access only by individuals possessing that ~~role~~pedigree certificate. The process is configured so that individual certificates can be generated and so that it can record those instances in which a given individual certificate was generated using this process. The recording can occur inside a database, a directory, or any other persistent data storage area, and is also labeled as a certificate policy OID in the certificate itself.

Please amend the paragraph beginning on page 18, line 17, as follows:

As a concrete example, assume that Alice Jones wishes to use an automated PKI registration process to generate her signature certificate. Alice obtains a hardware token from

her employer that has been factory pre-loaded with a ~~role~~pedigree certificate called "Level 3 Trust." Alice uses the hardware token to access the automated PKI registration process. If Alice were not able to present the "Level 3 Trust" certificate to the PKI registration process, the registration process would deny her attempt to generate an individual signature certificate. However, since Alice does have the requisite "Level 3 Trust" ~~role~~pedigree certificate, the PKI registration process consents to her request and more importantly, the PKI registration process knows that Alice must have used a hardware token to access the process. Accordingly, the PKI registration process can flag Alice's individual certificate as being a "Level 3" certificate in associated databases and directories. In other words, the pedigree of Alice's certificate has been successfully tracked automatically without requiring special intervention from another person. Furthermore, each certificate request must be specifically signed by the private key associated with the trust level of the certificate. This approach moves the "trust boundary" from the uncontrolled user computer to the controlled token itself.